Docket No. 299002053200
(PATENT)
Client Reference No. F5-01965232/01R00118-1US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Ichiro TOMOHIRO

Application No. 09/894,203 | Confirmation No. 7078

Filed: June 28, 2001 | Art Unit: 2136

For: SEMICONDUCTOR STORAGE DEVICE | Examiner: David G. Cervetti

AMENDED APPEAL BRIEF UNDER 37 CFR 41.37

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Notice of Non-Compliant Appeal Brief dated July 30, 2007, please replace applicant's original Appeal Brief with the following Amended Brief.

This is a timely appeal from the final rejection of claims 1-10 in this application.

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is Sharp Kabushiki Kaisha, the assignee of appellant's entire right, title and interest in this application.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences within the meaning of 37 CFR 41.37(c)(1)(ii) known to appellant or appellant's undersigned counsel.

III. STATUS OF CLAIMS

Claims 1-10 are pending in this application. Claims 1-10 stand finally rejected. The rejection of claims 1-10 is being appealed. The appealed claims are reproduced in the attached Appendix.

IV. STATUS OF AMENDMENTS

There are no pending amendments.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The invention relates to a semiconductor storage device 100, such as a flash memory device, having a security function for imposing limitation on data rewriting. The semiconductor storage device 100 comprises: at least one non-volatile memory cell array block 11 which is capable of receiving concurrent electrical erasure; a key means comprising a security release key; a lock means comprising a security registration lock corresponding to each of the at least one memory cell array block 11; at least one memory region 12, each one of said at least one memory region 12 being provided in the at least one memory cell array block 11, for storing the security release key; at least one nonvolatile storage means for storing the security registration lock (non-volatile registers 13); a determination circuit 14 for comparing a value which is generated based on the security release key against a value which is generated based on the security registration lock to determine whether or not to grant release of the security function (page 22, line 11, through page 23, line 2); and a memory cell array data output switching circuit 16 for, when an output signal from the determination circuit indicates a matching result of comparison between the value which is generated based on the security release key and the value which is generated based on the security registration lock, permitting data which is read from a corresponding one of the at least one memory cell array block 11 to be externally output (page 23, lines 12-19).

Appealed claims 1 and 3 recite features which may (or may not) be interpreted as means plus function limitations as permitted by 35 USC 112, sixth paragraph. In compliance with 37 CFR

41.37(c)(v), each claimed function is identified below and set forth with reference to the specification. While descriptions of the functions appear throughout the specification, appellants have attempted to identify representative sections of the specification.

Claim 1 recites "at least one nonvolatile storage means for storing the security registration lock." Descriptions of the nonvolatile storage means (non-volatile registers 13) may be found at: page 21, line 13, through page 23, line 19; page 31, lines 15-25; Figs. 1 and 2.

Claim 3 recites an "instruction interpretation means." Descriptions of the instruction interpretation means may be found at: page 26, line 14, through page 28, line 17.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-10 stand rejected under 35 USC 102(b) on Vicard (U.S. Patent No. 5,708,715).

VII. ARGUMENT

A. Vicard does not disclose storing both a key and a lock

Claims 1-10 stand rejected under 35 USC 102(b) on Vicard (U.S. Patent No. 5,708,715).

Vicard only discloses storing one element, regardless of which element (a key or a lock) is stored in Vicard, the other element is not stored. Vicard discloses a semiconductor memory incorporating a conventional data tamper prevention circuit similar to that depicted in appellant's Figure 3, and does not disclose or suggests "at least one memory region ... *for storing the security release key;* [and] *at least one non-volatile storage means for storing a security registration lock*" (emphasis added). Instead, the system of Vicard requires that a chip-key be supplied to a lock circuitry from a source external to the chip (Vicard, col. 4, lines 43-45).

The Examiner has asserted that "the key stored in hashed format is the release key since it is used to determine whether the circuit is to be unlocked or not. The hash, encrypted key is stored within the chip and a received encrypted key is submitted to the same hash function to later determine if a match exists (Vicard, summary of the invention, columns 3-6). ... Vicard clearly teaches having stored a hash of a key (a key on its own right)".

However, even if Vicard did disclose storing a key, Vicard does not disclose storing *both* a key and a lock as recited in claim 1. At best, Vicard only discloses storing a signature of a correct chip-key in the register 25 shown in Fig. 1 (see Vicard, col. 4, lines 62-66).

Vicard discloses inputting an external chip-key and decrypting the externally input chip-key at the secure communications module 20, such that a first intermediate chip-key output IV1 is sent to the one-way hash function module 26 to be hashed. The intermediate hashed chip-key IV2 is then compared to the stored signature of a correct chip-key at the comparator 27. While the Examiner asserts that the stored signature of Vicard discloses the security release key recited in claim 1, appellant respectfully submits that even if the stored signature were equivalent to the stored release key of claim 1, which it is not, Vicard would then fail to disclose or suggest storing the security registration lock in a nonvolatile storage, as recited in claim 1.

Additionally, the Examiner asserts that "Vicard teaches ref. value stored in storage means (col. 3, lines 20-30, i.e. semiconductor storage device)." Col. 3, lines 20-30 of Vicard discloses that "upon the comparison means detecting a hatch between the second intermediate value and a stored reference value, it provides the enable signal to the inhibit means of the functional block associated with the matches reference." In col. 2, lines 51-67 of Vicard, it is disclosed that "the lock circuitry comprises: storage means for storing at least, one reference value ... means for receiving the first intermediate value and for performing a one-way function on it to produce a second intermediate value" (emphasis added).

Accordingly, the stored reference value (indicated by the Examiner) is part of the "lock circuitry", and hence would represent a "lock" as noted above. Furthermore, the "second intermediate value" is not stored. Rather, the "second intermediate value" is produced from the received first intermediate value via a one-way function.

Vicard only discloses storing one element, the signature. Consequently, regardless of which element (a key or a lock) is stored in Vicard, a second element is not stored.

The Examiner responded to appellant's arguments that Vicard does not disclose the storing of a key by asserting in the second Advisory Action that "the key is input from externally, but an intermediate value (IV) is generated, and then this IV is used (see claim 1, and col. 3, lines 30-67). The IV value is stored and then used, clearly anticipating the chip-key being stored in the storage means."

Vicard discloses at col. 4, line 59 to col. 5, line 48, that: "When the secure communications block 20 is fed with an encrypted chip-key, it decrypts the chip-key and temporarily outputs the chip-key as first intermediate value IV1. ... The second measure taken to ensure the confidentiality of the chip-key, is that a copy of the chip-key is not stored as such in chip 10 for comparison against the input chip-key. Instead, a signature of the correct chip-key for the chip concerned is stored in register 25 of the lock circuitry ... the lock circuitry further comprises a one-way function block 26 that subjects the chip-key output as IV1 from block 20 to the one-way function ... used to form the chip-key signature held in register 25 [and] ... The resultant intermediate value IV2 output by block 26 is then compared in comparison block 27 with the signature stored in register 25."

Consequently, Vicard discloses that a signature of a chip-key is stored in the lock circuitry and therefore represents a "lock.". When a user enters a chip-key from an external source (i.e., the "key"), the input chip-key undergoes encryption and temporarily outputs the first intermediate value IV1. This IV1 is subjected to a one-way function (i.e., the same one-way function that produced the stored signature of the chip-key) to produce the second intermediate value IV2. Then, XV2 is compared with the signature of the chip-key that is stored in the lock circuitry (i.e., the "lock").

Appellant further notes that neither IV1 nor TV2 are stored, they are merely produced as a result of the externally input chip-key. Furthermore, it would not make sense to store the decrypted value IV1, since such an encrypted value may be accessed by physically accessing the device. As for storing IV2, Vicard does not actually disclose storing IV2 as it is merely output from the one-way function block 26.

B. The Examiner mistakenly equates comparing two keys with comparing a key to a lock

The Examiner asserts, in the Advisory Action mailed February 12, 2007, that appellant's arguments are unpersuasive because "Vicard teaches storing a signature of a correct chip-key and a decryption key, since the input is received in an encrypted form (col. 3, lines 40-50), decrypting the input to produce a first value, and applying a hash function to this value to produce a second value (col. 4, lines 43-61, and claims 1-6), Vicard further teaches using 2 or more chip-keys (col. 6, lines 20-36)."

By asserting that the hash encrypted key that is stored in the chip is the release key, and that a received encrypted key is submitted to the same hash function to later determine if a match exists, the Examiner takes the position that "a key" (the hash, encrypted key, as a release key) is compared with another "key" (received encrypted key). This interpretation is not consistent with the concept of a security "lock" and "key" configuration as disclosed and claimed by appellant, where a received "key" is compared with a stored "lock." In such configurations, when a received key matches a stored lock a security function is released. Instead, the Examiner appears to assert that a received "key" is compared with a stored "key," which is not what appellant claims

C. The Examiner has failed to address appellant's arguments that the chip-key of Vicard cannot correspond to the security release key

The Examiner has failed to address appellant's arguments that Vicard requires that the chip-key be externally supplied to the lock circuitry of the chip (see, e. g. , column 4, lines 43-45 of Vicard), i.e., *not* stored *in the chip.* The chip-key of Vicard cannot correspond to the security release key of this invention because, in Vicard, the chip-key is input by a user (from a source external to the chip) in contrast to the features of claim 1, where the security release key is stored in the at least one memory region, each one of said at least one memory region being provided in the at least one memory cell array block.

Vicard discloses that "[i]n order to ascertain whether an input chip-key is the correct one to unlock the particular chip 10 concerned, the lock circuitry further comprises a one-way function block 26 that subjects the chip-key output as IV1 from block 20 to the one-way function (in this case, the SHA) used to form the chip-key signature held in register 25. The resultant intermediate value hash encrypted key that is stored in the IV2 output by block 26 is then compared in comparison block 27 with the signature stored in register 25; if a match is found, the comparison block 27 outputs an enable signal on line 19 to cause operational enablement of the functional block 12." (Vicard, col. 5, lines 10-24).

In relation to claim 1, the signature of the chip-key of Vicard may correspond to the "security registration lock" that is stored in the at least one nonvolatile storage means (see appellant's Non-volatile register 13 of Figure 1 and paragraphs [0053] to [0055]).

As noted in appellant's specification, the conventional technique as shown in Figure 3 (which is noted above as being similar to the invention as disclosed by Vicard) has at least the following problems:

> First, in order to release the function limitation, it is necessary to externally input a function limitation release key. Accordingly, the above-described system *requires an external key storage device* for storing the function limitation release key. However, since the function limitation release key is retained external to the device, *the key must pass through an interfacing section every time access is requested, independent of what sort of encryption technique may be employed in the communication path between the devices*, i.e., between the device shown in FIG. 3 and any other device within the system (e.g., the key storage device). *This may run the risk of the function limitation release key being intercepted during communication, or being directly read from the external key storage device.*
>
> Moreover, *complicated circuitry is required for encrypting signals exchanged between devices*, and particularly complicated encryption is required. Hence, complicated decoding circuitry within the device is required to provide protection against repetitive attacks; and
>
> Furthermore, in order to effectuate a good tamper prevention function, merely replacing a given semiconductor storage device with a semiconductor storage device having a tamper prevention function does not suffice. In addition, *the entire system must be redesigned to enable a good tamper prevention function.*"

(Emphasis added). See, paragraphs [0009] to [0011] of appellant's specification; and col. 4, lines 43-61 of Vicard, wherein Vicard discloses the encryption and decryption that are required.

Furthermore, Examiner's assertion that the hash encrypted key that is stored within the chip is the claimed security release key is inconsistent with the teachings of Vicard and with the general concept of a "lock" and "key" arrangement as discussed above. To the contrary, it is pointed out that the hash encrypted key is stored in register 26 of the lock circuitry 11 of Vicard (Vicard, Fig. 1, and col. 4, line 65 to col. 5, line 9), such that Vicard does not disclose or suggest that the "key" (i. e., the security release key) is stored in the semiconductor storage device (i.e., in at least one memory region thereof).

VIII. CONCLUSION

For the forgoing reasons, appellant respectfully requests that the rejections of claims 1-10 be reversed.

In the event the U.S. patent and Trademark Office determines that an extension and/or other relief is required, appellant petitions for any required relief, including extensions of time, and authorize the Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to **Deposit Account No. 03-1952** referencing Attorney Docket No. **299002053200**.

Dated: August 8, 2007

Respectfully submitted,

By: Adam Keser
Registration No. 54,217
MORRISON & FOERSTER LLP
1650 Tysons Blvd, Suite 400
McLean, Virginia 22102
(703) 760-7301

APPENDIX OF CLAIMS

1. A semiconductor storage device having a security function for imposing limitation on data rewriting, the semiconductor storage device comprising:

at least one non-volatile memory cell array block which is capable of receiving concurrent electrical erasure;

a key means comprising a security release key;

a lock means comprising a security registration lock corresponding to each of the at least one memory cell array block;

at least one memory region, each one of said at least one memory region being provided in the at least one memory cell array block, for storing the security release key;

at least one nonvolatile storage means for storing the security registration lock;

a determination circuit for comparing a value which is generated based on the security release key against a value which is generated based on the security registration lock to determine whether or not to grant release of the security function; and

a memory cell array data output switching circuit for, when an output signal from the determination circuit indicates a matching result of comparison between the value which is generated based on the security release key and the value which is generated based on the security registration lock, permitting data which is read from a corresponding one of the at least one memory cell array block to be externally output.

2. A semiconductor storage device according to claim 1, wherein:

the semiconductor storage device further comprises at least one register for retaining an output signal output from the determination circuit; and

when an output signal output from the at least one register indicates that release of the security function is to be granted, the memory cell array data output switching circuit permits data

which is read from a corresponding one of the at least one memory cell array block to be externally output.

3. A semiconductor storage device according to claim 1, further comprising instruction interpretation means for interpreting an externally-input setting instruction to write at least one of the security release key and the security registration lock into the at least one memory region or the at least one non-volatile storage means, respectively.

4. A semiconductor storage device according to claim 2, wherein the determination circuit compares the value which is generated based on the security release key against the value which is generated based on the security registration lock for each of the at least one memory cell array block, and results of comparison are collaterally written in the at least one register.

5. A semiconductor storage device according to claim 1, further comprising a unidirectional conversion circuit or an encryption circuit, wherein results of converting the security release key and the security registration lock by means of the unidirectional conversion circuit or the encryption circuit are written to the at least one memory region and the at least one non-volatile storage means, respectively.

6. A semiconductor storage device according to claim 1, which lacks means for reading the security release key and the security registration lock.

7. A semiconductor storage device according to claim 1, wherein:

the at least one non-volatile storage means is a one-time programmable Read Only Memory which prohibits rewriting and erasure; and

rewriting and erasure are prohibited after the security registration lock is written.

8. A semiconductor storage device according to claim 1, wherein:

the at least one non-volatile storage means is a one-time programmable Read Only Memory which prohibits rewriting and erasure; and

the semiconductor storage device has a non-volatile lock function for locking the semiconductor storage device to prohibit rewriting and erasure after writing of the security registration lock has been performed.

9. A semiconductor storage device according to claim 1, further comprising a flag indicating that the security release key has been set,

wherein the flag is set automatically or manually after the security release key is written, thereby prohibiting additional writing to the corresponding one of the at least one memory cell array block.

10. A semiconductor storage device according to claim 1, wherein a wait operation is performed while writing the security release key to the at least one memory region.

EVIDENCE APPENDIX

[NONE]

RELATED PROCEEDINGS APPENDIX

[NONE]